Programma van Eisen

Door het indienen van een inschrijving voor deze aanbesteding verklaart de inschrijver zich onvoorwaardelijk en volledig akkoord met de in dit Programma van Eisen opgenomen eisen. Eventuele kosten die voortvloeien uit het voldoen aan deze eisen worden geacht volledig te zijn inbegrepen in de prijsopgave van de inschrijver. Deze eisen kunnen niet leiden tot aanvullende of extra kosten.

Definities van begrippen die in dit Programma van Eisen met een hoofdletter zijn geschreven, zijn opgenomen in de Overeenkomst.

Eisen kunnen vanuit hun doelgebied op meerdere plaatsen worden benoemd en/of nader zijn uitgewerkt in de Overeenkomst. In geval van tegenstrijdigheid prevaleert het Programma van Eisen, tenzij OPDRACHTGEVER schriftelijk anders bepaalt.

Algemene eisen

Eis-ID	Eis
ALG-1.	Medewerkers van OPDRACHTNEMER (en ingeschakelde derden) die werkzaamheden verrichten op locaties van OPDRACHTGEVER houden zich te allen tijde aan de geldende huisregels en volgen aanwijzingen van daartoe bevoegde SRL-medewerkers op. Zij kunnen zich op eerste verzoek legitimeren. In geval van calamiteiten worden instructies van de BHV-organisatie van OPDRACHTGEVER onverwijld opgevolgd.
ALG-2.	OPDRACHTNEMER handelt conform de AVG en overige toepasselijke privacywetgeving. Partijen sluiten vóór aanvang van de verwerking een verwerkersovereenkomst (DPA), op basis van de meest recente modelverwerkersovereenkomst van het Privacyconvenant Onderwijs (versie conform actuele stand). OPDRACHTNEMER verwerkt persoonsgegevens uitsluitend op schriftelijke instructie van OPDRACHTGEVER en verstrekt deze niet aan derden, behoudens voor zover wettelijk toegestaan of verplicht. OPDRACHTGEVER behandelt door OPDRACHTNEMER verstrekte vertrouwelijke informatie eveneens vertrouwelijk. http://www.privacyconvenant.nl/
ALG-3.	Toegang tot locaties van OPDRACHTGEVER vindt uitsluitend plaats na voorafgaand overleg met OPDRACHTGEVER en, indien OPDRACHTGEVER dit verlangt, onder begeleiding van een door OPDRACHTGEVER aangewezen medewerker. OPDRACHTNEMER kondigt gewenste aanwezigheid op een SRL-locatie tijdig vooraf aan bij de afdeling ICT (of een door OPDRACHTGEVER aangewezen contactpunt).
ALG-4.	Alle medewerkers van OPDRACHTNEMER en door OPDRACHTNEMER ingeschakelde derden die werkzaamheden op locatie van OPDRACHTGEVER uitvoeren beschikken over een geldige VOG passend bij de onderwijscontext en kunnen zich identificeren. De VOG wordt op eerste verzoek overgelegd en is op het moment van start van de werkzaamheden maximaal drie (3) maanden oud
ALG-5.	OPDRACHTNEMER informeert OPDRACHTGEVER gedurende de looptijd proactief over relevante ontwikkelingen die impact (kunnen) hebben op de DLWO-dienstverlening, waaronder wijzigingen in Microsoft-diensten, security-ontwikkelingen, end-of-life aankondigingen en majeure roadmap-wijzigingen. OPDRACHTNEMER doet hiertoe minimaal per kwartaal een schriftelijke update met impactanalyse en advies.
ALG-6.	Op locaties van OPDRACHTGEVER waar een telefoonverbod geldt in ruimtes waar leerlingen aanwezig zijn, houdt OPDRACHTNEMER hier rekening mee bij de uitvoering van de werkzaamheden en volgt de geldende huisregels.
ALG-7.	SRL beschikt over een Beveiligings- en Continuïteitsplan, inclusief risicoanalyse en passende technische en organisatorische maatregelen. OPDRACHTGEVER actualiseert dit plan jaarlijks. OPDRACHTNEMER neemt hiervan kennis, handelt conform dit plan voor zover van toepassing op de dienstverlening en signaleert afwijkingen, risico's of noodzakelijke maatregelen proactief aan OPDRACHTGEVER.
ALG-8.	Beveiligings- en Continuïteitsplan (waarin een risicoanalyse en passende technische en organisatorisch maatregelen worden genomen om beveiligings- en continuïteitsrisico's te mitigeren) opgesteld. Deze plannen worden jaarlijks bijgewerkt. OPDRACHTNEMER neemt hier hoogte van en handelt hiernaar.

M365 Basisvoorzieningen

Eis-ID	Eis
M365-1.	Er is één centrale Microsoft 365 tenant ingericht die alle scholen en het Centraal Service Bureau ondersteunt.
M365-2.	De tenant ondersteunt meerdere domeinen zodat scholen een eigen identiteit, zoals een eigen e-maildomein, kunnen gebruiken binnen één tenant.
M365-3.	De tenantinrichting is schaalbaar zodat nieuwe scholen, gebruikers en diensten zonder herontwerp kunnen worden toegevoegd.
M365-4.	Voor de centrale Microsoft 365-omgeving is een baseline-inrichting vastgesteld, toegepast en beheerd conform het Architectuurkader. Voor nieuwe of aanvullende clouddiensten stelt OPDRACHTNEMER vóór ingebruikname een passende baseline op, legt deze ter goedkeuring voor aan OPDRACHTGEVER en past deze na akkoord toe.
M365-5.	OPDRACHTNEMER legt afwijkingen van de vastgestelde baselines vast, gemotiveerd en beheerst binnen centrale governance.
M365-6.	OPDRACHTNEMER adviseert periodiek over noodzakelijke aanpassingen van baselines als gevolg van nieuwe dreigingen of ontwikkelingen.
M365-7.	Van de OPDRACHTNEMER wordt verwacht dat Configuratie- en wijzigingsbeheer voor tenant- en workloadinstellingen is ingericht, inclusief impactanalyse, logging en herstelmogelijkheden.
M365-8.	Wijzigingen met impact op beschikbaarheid, security of gebruikerservaring worden door OPDRACHTNEMER vooraf afgestemd met de OPDRACHTGEVER.
M365-9.	Instellingen voor externe samenwerking en het delen van informatie zijn organisatiebreed uniform ingericht voor SharePoint, OneDrive en Teams. Differentiatie per doelgroep vindt uitsluitend plaats op basis van centrale besluitvorming.
M365-10.	Externe deling en samenwerking zijn aantoonbaar beheerst door logging, periodieke controles en rapportages.
M365-11.	De inrichting en het beheer van de Microsoft 365 omgeving houdt rekening met beschikbaarheid en continuïteit passend bij gebruik binnen het onderwijs.
M365-12.	Back-up en herstel van Microsoft 365-data zijn ingericht en worden periodiek (minimaal jaarlijks) getest conform met OPDRACHTGEVER overeengekomen kaders (scope, RPO/RTO, retentie en rapportage)
M365-13.	OPDRACHTNEMER levert maandelijks een rapportage met minimaal: (i) uitgevoerde wijzigingen, (ii) incidenten (aantallen, doorlooptijden, trends), en (iii) openstaande problemen/risico's.
M365-14.	Periodieke rapportages (minimaal per kwartaal) geven inzicht in baseline compliance en verbetermaatregelen.
M365-15.	Rapportages zijn geschikt voor gebruik door de OPDRACHTGEVER en bevatten operationele en tactische inzichten.
M365-16.	OPDRACHTNEMER ondersteunt bij het beheer en de optimalisatie van Microsoft 365 en eventuele Azure-licenties, inclusief inzicht in gebruik, kosten en verbetermogelijkheden, en rapporteert periodiek over licentiegebruik en kostenontwikkelingen met advies over optimalisatie.
M365-17.	OPDRACHTNEMER realiseert en beheert koppelingen met door OPDRACHTGEVER aangewezen systemen binnen scope. OPDRACHTGEVER verstrekt hiervoor tijdig een lijst met systemen, prioritering en eisen. Nieuwe of gewijzigde koppelingen worden ingericht conform het afgesproken wijzigingsproces.

M365-18.	OPDRACHTNEMER geeft gevraagd en ongevraagd advies om de Microsoft 365-tenant up-to-date te houden, onderbouwd met relevante rapportages en impactanalyse

DLWO

Eis-ID	Eis
DLWO-1.	OPDRACHTNEMER levert en beheert de DLWO als samenhangend dienstconcept voor leerlingen, leerkrachten en onderwijs ondersteunend personeel, inclusief de in scope beschreven gebruiksscenario's.
DLWO-2.	Er is een doelgroepbewuste portaalfunctie beschikbaar als startomgeving, met rolgestuurde ontsluiting van applicaties en diensten voor leerlingen en medewerkers.
DLWO-3.	Leerlingtoegang is primair browser-gebaseerd en ondersteunt gebruik op eigen apparaten, zonder noodzaak voor lokale installatie van applicaties voor basisgebruik van de DLWO.
DLWO-4.	De DLWO ondersteunt meerdere scenario's, leerling browser-toegang, beheerde leerlingwerkplekken voor computerlokalen, beheerde toets of examenwerkplekken, en beheerde werkplekken voor medewerkers, met per scenario passende beleids- en beveiligingsinstellingen.
DLWO-5.	Toegang tot aangesloten applicaties wordt via gestandaardiseerde toegangsmethoden ingericht, waaronder Single Sign On waar mogelijk, met rol- of groepgestuurde toegang.
DLWO-6.	Externe gebruikers kunnen binnen de DLWO samenwerken op basis van een centraal beheerst toegangsmodel, passend bij de rol en autorisatie van de externe gebruiker.
DLWO-7.	OPDRACHTNEMER ondersteunt gebruik van de DLWO met gebruikersgerichte ondersteuning, zoals instructies, FAQ's of handleidingen, afgestemd op leerlingen en medewerkers.
DLWO-8.	De DLWO wordt zodanig beheerd, dat beschikbaarheid en performance aantoonbaar passend zijn voor onderwijsgebruik, inclusief inzicht in verstoringen, trends en capaciteitsontwikkeling.
DLWO-9.	De DLWO is ingericht volgens het principe van veilige toegang, waarbij toegang tot diensten en data aantoonbaar is geborgd met passende beleids- en beveiligingsmaatregelen uit het Architectuurkader.
DLWO-10.	OPDRACHTNEMER stemt de DLWO-dienstverlening aantoonbaar af met applicatieleveranciers en overige leveranciers binnen de keten, zodat samenhang en beschikbaarheid geborgd blijven.
DLWO-11.	OPDRACHTNEMER richt governance in voor Teams, Microsoft 365 groepen en SharePoint sites, zodat aanmaak, eigenaarschap, naamgeving en lifecycle beheerst plaatsvinden en wildgroei wordt voorkomen, passend binnen de centrale governance.
DLWO-12.	De DLWO ondersteunt een beheersbare samenwerkingsstructuur waarbij Teams en bijbehorende opslag logisch aansluiten op de organisatie, zoals school, afdeling, project of functie, inclusief afspraken over eigenaarschap.
DLWO-13.	OPDRACHTNEMER hanteert voor beheerde medewerkerswerkplekken onderhoudsvensters die verstoring van onderwijsprocessen minimaliseren. Functionele updates en herstarts worden zoveel mogelijk buiten lesuren gepland. Indien onderhoud tijdens schooluren noodzakelijk is (bijv. kritieke beveiligingspatch), wordt dit vooraf afgestemd met OPDRACHTGEVER en tijdig gecommuniceerd. OPDRACHTNEMER stelt, op basis van door OPDRACHTGEVER aangeleverde informatie, een jaarlijkse onderhoudskalender op en actualiseert deze indien nodig.

IAM

Eis-ID	Eis
IAM-1.	Authenticatie en autorisatie voor de in scope omgeving zijn centraal ingericht via Microsoft Entra ID (Identity Provider).
IAM-2.	Multi-factor authenticatie is verplicht voor alle accounts, inclusief externe gebruikers. Uitzonderingen zijn beperkt, gemotiveerd en vastgelegd via centrale governance.
IAM-3.	Conditional Access is ingericht als baseline voor toegangsbeleid, waarbij minimaal rekening wordt gehouden met locatie, apparaatstatus en risicoprofiel. Uitrol vindt gecontroleerd plaats om verstoring van het onderwijsproces te voorkomen.
IAM-4.	Autorisaties zijn ingericht op basis van rollen en groepen, volgens het principe van minimale rechten (least privilege).
IAM-5.	Beheeraccounts en verhoogde rechten zijn aanvullend beveiligd, gescheiden van reguliere accounts en centraal beheerst. Noodtoegang (break-glass) is ingericht en periodiek getoetst.
IAM-6.	Externe toegang voor onder andere MR-leden, externe inhuur en leveranciers is centraal beheersbaar ingericht, inclusief logging, tijdelijkheid en aantoonbare intrekking van rechten bij beëindiging van de toegang.
IAM-7.	Single Sign-On (SSO) is ingericht voor aangesloten applicaties waar mogelijk, met een aantoonbaar beheerst alternatief proces indien SSO aantoonbaar niet mogelijk is.
IAM-8.	Toegangsverlening en wijzigingen in rechten zijn centraal gelogd en herleidbaar, inclusief vastlegging van wie heeft aangevraagd en wie heeft goedgekeurd (audittrail).
IAM-9.	Afwijkingen op IAM-baselines en uitzonderingen op beleid zijn centraal beheerst, traceerbaar en periodiek toetsbaar binnen de governance.
IAM-10.	Er is een periodiek herbeoordelingsproces van toegangsrechten ingericht voor gevoelige rollen, beheerfuncties en externe toegang, inclusief aantoonbare bewijsvoering door middel van rapportages of steekproeven.
IAM-11.	Privileged Identity Management wordt toegepast voor het tijdelijk activeren van verhoogde rechten, inclusief logging en voorafgaande goedkeuring conform governance.
IAM-12.	Voor schoollocaties of organisatieonderdelen van OPDRACHTGEVER die gebruikmaken van Google Workspace, richt OPDRACHTNEMER federatie in tussen Google Workspace en Microsoft Entra ID, zodat authenticatie centraal via Entra ID plaatsvindt en gebruikers met hun centrale identiteit toegang krijgen tot Google Workspace.

IGA

Eis-ID	Eis
IGA-1.	Provisioning van accounts en rechten voor medewerkers is gebaseerd op een HR-bronsysteem (AFAS), aangevuld met eventueel andere bronnen.
IGA-2.	Provisioning van accounts en rechten voor leerlingen is gebaseerd op een leerlingadministratiesysteem (Somtoday en/of Parnassys).
IGA-3.	Er is een lifecycleproces ingericht voor instroom, doorstroom en uitstroom voor medewerkers en leerlingen, inclusief automatische of gecontroleerde deprovisioning bij uitdiensttreding/uitschrijving. Termijnen voor (de)provisioning worden vastgelegd en periodiek gerapporteerd.
IGA-4.	Accounts en basisattributen in Entra ID worden automatisch of gecontroleerd aangemaakt, gewijzigd en beëindigd op basis van brondata.
IGA-5.	Groeps- en roltoekenningen worden beheerst uitgevoerd op basis van vastgestelde autorisatieregels die zijn afgeleid van brondata (bijvoorbeeld school, rol, afdeling, klas).
IGA-6.	Waar applicaties dit ondersteunen, wordt automatische account- en autorisatieprovisioning ingericht op basis van open standaarden (bij voorkeur SCIM) of aantoonbaar gelijkwaardig.
IGA-7.	Indien automatische provisioning aantoonbaar niet mogelijk is, wordt een beheerst alternatief proces ingericht voor account- en autorisatiehandelingen, inclusief traceerbaarheid en periodieke controle.
IGA-8.	De inrichting ondersteunt tijdelijke identiteiten buiten de bronsystemen wanneer dit noodzakelijk is voor de bedrijfsvoering, inclusief verplichte einddatum en automatische beëindiging.
IGA-9.	Provisioningkoppelingen met bronsystemen en applicaties zijn beheersbaar, inclusief statusinzicht, foutmeldingen en de mogelijkheid om synchronisaties gecontroleerd te starten of te herstellen.
IGA-10.	Alle provisioninghandelingen (aanmaken/wijzigen/beëindigen accounts en rechten) zijn gelogd en herleidbaar tot bron, actor en tijdstip.
IGA-11.	IAM/IGA-uitzonderingen en handmatige account- of autorisatiehandelingen worden geregistreerd in de ITSM-tooling van SRL, zodat besluitvorming en uitvoering traceerbaar zijn.
IGA-12.	Er is een gestandaardiseerd aansluitproces voor nieuwe applicaties op IAM/IGA, inclusief afspraken over SSO, provisioning en autorisatiebeheer.
IGA-13.	De inrichting ondersteunt interpretatie en transformatie van brondata naar doelsystemen (mapping), zodat autorisaties en attributen eenduidig en reproduceerbaar worden verwerkt.
IGA-14.	Bij fouten in provisioning of synchronisatie worden automatisch beheersmaatregelen toegepast (zoals pauzeren van verwerking en alerteren), zodat foutieve of incomplete provisioning wordt voorkomen.
IGA-15.	De inrichting ondersteunt het tijdelijk delegeren van bevoegdheden en/of rechten (mandatering), inclusief traceerbaarheid, einddatum en logging.
IGA-16.	Het proces voor periodieke herbeoordeling van rechten (attestatie) is workflowmatig ingericht, inclusief logging van besluiten en rapportage.

IGA-17.	De inrichting ondersteunt het vooraf simuleren en inzichtelijk maken van het effect van wijzigingen in brondata, autorisatieregels, mappings en provisioningregels op accounts, groepen en rechten (IST/SOLL), zodat fouten en ongewenste autorisaties vóór uitvoering worden voorkomen.
IGA-18.	Tijdelijke identiteiten kunnen beheerst worden aangemaakt buiten bronsystemen wanneer dit noodzakelijk is voor de bedrijfsvoering, inclusief verplichte motivatie, eigenaar en einddatum.
IGA-19.	Tijdelijke identiteiten kunnen beheerst worden gepauzeerd/uitgeschakeld en hersteld, inclusief logging en herleidbaarheid.
IGA-20.	Voor tijdelijke identiteiten geldt dat provisioning en deprovisioning aantoonbaar wordt uitgevoerd voor zowel Entra ID als gekoppelde applicaties waar van toepassing.
IGA-21.	De provisioning-inrichting bevat eenduidige match- en correlatieregels om identiteiten uit bronsystemen correct te koppelen aan bestaande accounts in Entra ID, zodat dubbele accounts aantoonbaar worden voorkomen.
IGA-22.	Bij twijfelachtige matches, conflictsituaties of mogelijke dubbele identiteiten wordt provisioning beheerst afgehandeld (bijvoorbeeld via uitval/quarantaine), inclusief melding, traceerbare besluitvorming en gecontroleerde correctie.
IGA-23.	De provisioning van Microsoft 365-groepen, Teams-omgevingen en/of Google Workspace wordt geautomatiseerd ingericht op basis van betrouwbare brondata (bijvoorbeeld klas-, groeps- of organisatiestructuurinformatie), inclusief automatische toewijzing van bijbehorende rechten.
IGA-24.	Het lifecycleproces is centraal beheerd, auditbaar en gekoppeld aan informatieclassificatie en retentiebeleid.

Endpointmanagement

Eis-ID	Eis
EP-1.	OPDRACHTNEMER levert en beheert een centrale endpoint managementoplossing voor beheerde Windows werkplekken, met beleidsafdwinging, compliance monitoring en rapportage.
EP-2.	De endpoint managementoplossing ondersteunt minimaal beheerde Windows werkplekken voor medewerkers en beheerde Windows leerlingwerkplekken, inclusief scenario's voor computerlokaal en toets of examen.
EP-3.	Zero touch provisioning is mogelijk voor beheerde Windows werkplekken, met standaard inrichting zonder handmatige basisconfiguratie per device.
EP-4.	Toegang tot bedrijfsresources voor beheerde Windows werkplekken is gekoppeld aan apparaatcompliance, met centraal afdwingbaar beleid.
EP-5.	Beheerde Windows werkplekken worden ingericht conform vastgestelde hardening en baseline instellingen, passend bij het Architectuurkader en onderwijsgebruik.
EP-6.	Patch en updatebeheer is centraal ingericht met inzicht in update status en met een beheerst uitzonderingsproces.
EP-7.	Patch- en updatebeheer is centraal ingericht met inzicht in patchstatus en een beheerst uitzonderingsproces. Patchtermijnen zijn vastgesteld en worden gerapporteerd, met prioritering op kwetsbaarheid en impact. Kritieke beveiligingspatches worden binnen een overeengekomen maximale doorlooptijd uitgerold, met expliciete escalatie bij afwijkingen.
EP-8.	Technisch applicatiebeheer is ingericht, inclusief centrale uitrol en onderhoud van applicaties zonder lokale adminrechten voor standaardgebruikers.
EP-9.	Indien een third party beheeroplossing wordt ingezet, werkt deze aantoonbaar integraal samen met Microsoft 365 en ondersteunt deze de benodigde security en compliance handhaving.
EP-10.	Beheerde Windows werkplekken leveren logging en telemetrie op die geschikt is voor beheer, troubleshooting en incidentanalyse.
EP-11.	Er is Defender endpoint beveiliging ingericht met detectie en responsmogelijkheden passend bij de risico's en het volwassenheidsniveau van de organisatie.
EP-12.	Configuraties worden centraal beheerd en wijzigingen zijn herleidbaar, inclusief versiebeheer of aantoonbare registratie van beleidswijzigingen.
EP-13.	Voor toets of examenwerkplekken is een apart beheersprofiel mogelijk, met passende beperkingen en beheersmaatregelen voor integriteit van toetsing.
EP-14.	Beheerde Windows werkplekken functioneren veilig op schoollocaties en daarbuiten, met passend toegangsbeleid en configuraties.
EP-15.	Periodieke rapportages bevatten minimaal inzicht in compliance, patchstatus, kwetsbaarheden, en afwijkingen op baselines.
EP-16.	Runbooks, standaardconfiguraties en beleidssets voor werkplekbeheer zijn gedocumenteerd en overdraagbaar aan de OPDRACHTGEVER.

EP-17.	Kritieke beveiligingspatches worden binnen zeven (7) kalenderdagen geïnstalleerd, tenzij OPDRACHTGEVER schriftelijk anders besluit op basis van aantoonbare risico-afweging
EP-18.	Er is een proces voor software aanvragen (automatische installatie bij aanvrager na goedkeuringsproces)
EP-19.	De oplossing ondersteunt registratie en uitrol van nieuwe devices via hardwareleveranciers (o.a. Dell, Dustin) door middel van Windows Autopilot (of aantoonbaar gelijkwaardig), inclusief koppeling met de centrale endpoint managementomgeving.

Servicemanagement

Eis-ID	Eis
SM-1.	OPDRACHTNEMER levert beheer en ondersteuning voor de in scope basisvoorzieningen en de DLWO gedurende de contractperiode, inclusief ketenafstemming met betrokken leveranciers.
SM-2.	Er is één centraal aanspreekpunt voor incidenten, serviceverzoeken en wijzigingen, met duidelijke routering en escalatie (hierna verder genoemd als Servicedesk).
SM-3.	Bereikbaarheid, supportvensters en escalatieafspraken zijn vastgelegd en passend bij onderwijsgebruik.
SM-4.	OPDRACHTNEMER biedt op werkdagen (maandag t/m vrijdag) telefonisch support voor ICT-medewerkers via de servicedesk van 08:00 tot 17:00 uur.
SM-5.	Incidentmanagement is ingericht met prioriteiten, responstijden en oplostijden, inclusief communicatie bij verstoringen.
SM-6.	Er is probleemmanagement ingericht om herhalende verstoringen structureel te analyseren, op te lossen en te voorkomen.
SM-7.	Changemanagement is ingericht, inclusief impactanalyse, planning, communicatie, rollback (herstel) en vastlegging van wijzigingen.
SM-8.	Onderhoudsvensters en releasemanagement zijn ingericht zodat verstoring van onderwijsprocessen wordt geminimaliseerd.
SM-9.	Periodieke rapportages geven inzicht in incidenten, changes, performance, compliance en verbetermaatregelen, passend voor regiesturing.
SM-10.	Er vindt periodiek overleg plaats met de OPDRACHTGEVER over prestaties, risico's, verbeteracties en roadmap.
SM-11.	Operationele documentatie, runbooks en beheerprocedures zijn actueel en beschikbaar voor de OPDRACHTGEVER.
SM-12.	De OPDRACHTNEMER coördineert incidenten en wijzigingen over de keten, inclusief afstemming met applicatieleveranciers en netwerkleveranciers waar relevant.
SM-13.	De OPDRACHTNEMER levert proactieve adviezen en een verbeteragenda gericht op stabiliteit, security, compliancy en onderwijsontwikkelingen.
SM-14.	De OPDRACHTNEMER ondersteunt zelfredzaamheid met kennisartikelen, FAQ's en/of self service waar passend, ter ontlasting van de servicedesk.
SM-15.	Er is een kwaliteitsborgingsmechanisme ingericht, inclusief monitoring, trendanalyse en structurele verbetermaatregelen.
SM-16.	De OPDRACHTNEMER werkt aantoonbaar mee aan overdracht en exit, inclusief overdraagbare documentatie, configuratieoverzichten en kennisoverdracht.
SM-17.	De OPDRACHTNEMER maakt expliciet welke werkzaamheden wel binnen de dienstverlening vallen en welke randvoorwaarden gelden, zodat de aanbestedende dienst de eigen verantwoordelijkheden kan organiseren en risico's kan beheersen.

SM-18.	OPDRACHTNEMER sluit aan op de ITSM-tooling van OPDRACHTGEVER als single point of truth voor incidenten, serviceverzoeken en wijzigingen. OPDRACHTNEMER realiseert een werkende koppeling en werkwijze waarbij meldingen vanuit OPDRACHTGEVER worden doorgezet naar 2e en 3e lijn, en statusupdates, voortgang en afsluiting aantoonbaar worden terug geregistreerd zodat volledige tickettraceerbaarheid is geborgd.
SM-19.	OPDRACHTNEMER zet voor de dienstverlening een herkenbare en zoveel mogelijk vaste supportpool in. Communicatie richting gebruikers en OPDRACHTGEVER vindt plaats in het Nederlands en voor de internationale scholen en afdelingen in het Engels. OPDRACHTNEMER houdt bij inrichting van supportprocessen rekening met de context van het onderwijs, waaronder bereikbaarheid tijdens schooltijden en piekmomenten.
SM-20.	OPDRACHTNEMER beschikt over een ingericht major incident- en crisisproces. Bij verstoringen met hoge impact worden aangewezen key users en de OPDRACHTGEVER actief en periodiek geïnformeerd over status, impact en herstelmaatregelen.
SM-21.	OPDRACHTNEMER meet periodiek de tevredenheid van eindgebruikers over de dienstverlening en bespreekt de uitkomsten met de regieorganisatie, inclusief concrete verbeteracties.
SM-22.	OPDRACHTNEMER kan op afroep ondersteuning op locatie leveren voor werkzaamheden die niet remote kunnen worden uitgevoerd, zoals hardwarevervanging, aansluitingen en overige praktische ondersteuning, binnen vooraf afgesproken kaders.
SM-23.	OPDRACHTNEMER levert ondersteuning in zowel Nederlands als Engels, met minimaal servicedocumentatie in NL/EN voor kernprocedures.
SM-24.	Het intellectueel eigendom van specifiek voor OPDRACHTGEVER ontwikkelde documentatie, configuraties en maatwerkinrichting berust bij OPDRACHTGEVER. OPDRACHTNEMER stelt bij contracteinde een overzicht op en draagt deze zonder aanvullende kosten over.
SM-25.	Servicedesk van OPDRACHTNEMER is onder één telefoonnummer bereikbaar
SM-26.	Standaard wijzigingen worden uitgevoerd op basis van vastgestelde procedures en zijn inbegrepen in de dienstverlening.
SM-27.	De wijze van het in stand houden van de geleverde functionaliteit met preventief, correctief en adaptief onderhoud gebeurt op kosten van Opdrachtnemer.
SM-28.	Indien er een niet standaard wijziging wordt uitgevraagd (RfC) of het uitvoeren van een standaard wijziging niet mogelijk is, zal OPDRACHTNEMER binnen 5 werkdagen met een Proposal for Change (PfC) komen wanneer deze wel gerealiseerd kan worden, waarbij er een plan van aanpak wordt gemaakt om deze wijziging te realiseren, inclusief de bijbehorende kosten, impactanalyse en doorlooptijd. Niet standaard wijzigingen worden in het Change Advisory Board (CAB) besproken. Goedkeuring op basis van PfC wordt door OPDRACHTGEVER gegeven. Daarna zal OPDRACHTNEMER binnen de afgesproken termijn de wijziging doorvoeren.
SM-29.	Indien OPDRACHTGEVER een wijziging bekend maakt die zowel OPDRACHTNEMER als andere leverancier betreft, zal OPDRACHTNEMER hier het voortouw in nemen, voor het uitvoeren van deze wijziging. Eventuele offertes en kosten voor wat betreft andere leverancier wordt rechtstreeks met OPDRACHTGEVER en andere leverancier besproken en afgehandeld, eventueel in overleg met OPDRACHTNEMER.
SM-30.	OPDRACHTGEVER kan buiten de standaard werkdagen ook extra supportmomenten aanvragen, bijvoorbeeld bij open dagen of ouderavonden.

SM-31.	OPDRACHTNEMER is Single Point of Contact (SPoC) voor onder andere de (applicatie)leveranciers en afdeling functioneel beheer
SM-32.	OPDRACHTNEMER werkt met een systematische prioritering van tickets op basis van urgentie en impact op het proces van de SRL
SM-33.	OPDRACHTNEMER organiseert op verzoek voor OPDRACHTGEVER kennissessies voor gebruikers / IT-ondersteuners / keyusers om de vraag naar eerstelijnsondersteuning te verminderen. Dit proces wordt nader afgestemd met OPDRACHTGEVER.
SM-34.	OPDRACHTNEMER faciliteert het voorbereiden en uitvoeren van communicatie in geval van grote IT-projecten en -incidenten.
SM-35.	Voor spoedgevallen (calamiteiten en/of storingen buiten de aangeboden openingstijden van de servicedesk van IT-leverancier) is een storingsnummer / noodnummer beschikbaar, inclusief escalatie naar OPDRACHTGEVER voor het oplossen van incidenten.
SM-36.	Indien OPDRACHTNEMER een melding niet zelfstandig kan oplossen, wordt dit uiterlijk binnen 4 uur na ontvangst doorgezet naar de verantwoordelijke partij.
SM-37.	In geval van een IT crisis/P1 neemt OPDRACHTNEMER de kartrekkers rol op zich, tenzij OPDRACHTGEVER hier op dat moment anders over beslist. OPDRACHTNEMER is actief lid en zorgt voor de communicatie in overleg met OPDRACHTGEVER
SM-38.	In geval van een IT crisis/P1 neemt OPDRACHTNEMER binnen 1 uur contact op met OPDRACHTGEVER om de impact te bepalen en gevolgen in te schatten. Daarna wordt besloten hoe snel een crisisteam wordt opgezet.
SM-39.	OPDRACHTGEVER kan prioriteit opschalen bij OPDRACHTNEMER
SM-40.	OPDRACHTNEMER levert een RACI-matrix voor de activiteiten, inclusief afstemming wie verantwoordelijk is voor het omzetten van werkplekken per locatie, en hoe samenwerking plaatsvindt met interne ICT van OPDRACHTGEVER en eventuele huidige leveranciers.
SM-41.	OPDRACHTNEMER levert een voorstel voor een XLA (eXperience Level Agreement) en DAP, waarbij naast proces en techniek expliciet de gebruikerservaring wordt meegenomen, inclusief meetmethodiek.

Implementatie en Adoptie

Eis-ID	Eis
IMP-1.	OPDRACHTNEMER levert een implementatie- en transitieaanpak die aansluit op de scope, inclusief fasering, afhankelijkheden, risico's en governance.
IMP-2.	OPDRACHTNEMER bouwt de beoogde omgeving volgens de afgesproken aanpak en uitgangspunten, met traceerbare keuzes en vastlegging van afwijkingen.
IMP-3.	Migratie of herinrichting van relevante onderdelen van de huidige omgeving wordt gecontroleerd uitgevoerd, met minimale verstoring van onderwijsprocessen.
IMP-4.	Acceptatiecriteria voor oplevering zijn vooraf vastgesteld, inclusief testgevallen voor de belangrijkste scenario's en ketens.
IMP-5.	Integraties met geprioriteerde applicaties worden gerealiseerd en aantoonbaar getest volgens afgesproken aansluit- en testmethodiek.
IMP-6.	Bij oplevering voldoen inrichting en configuraties aantoonbaar aan de afgesproken baselines en kernmaatregelen uit het Architectuurkader, inclusief vastlegging van uitzonderingen.
IMP-7.	OPDRACHTNEMER richt beheerprocessen in voordat de omgeving naar beheer gaat, inclusief incident, change, rapportage en ketenafstemming.
IMP-8.	Oplevering omvat complete en overdraagbare documentatie, inclusief configuratie-overzichten, runbooks, beheersafspraken en relevante ontwerpen.
IMP-9.	Er vindt een gecontroleerde overdracht plaats naar de regieorganisatie, inclusief kennisoverdracht, contactstructuur en afspraken over samenwerking.
IMP-10.	Na initiële oplevering is een stabilisatieperiode ingericht waarin verstoringen versneld worden opgepakt en structureel verbeterd.
IMP-11.	Tijdens implementatie wordt periodiek voortgang gerapporteerd met inzicht in planning, risico's, issues en besluiten.
IMP-12.	OPDRACHTNEMER levert een migratieplan waarin per domein is uitgewerkt wat wordt gemigreerd of opnieuw ingericht, ten minste bestaande uit accounts, autorisaties, mailboxen, SharePoint- en Teams-data, OneDrive-data, werkplekken en relevante configuraties, inclusief afhankelijkheden, risico's en randvoorwaarden.
IMP-13.	OPDRACHTNEMER levert een RACI-matrix voor migratieactiviteiten, inclusief afstemming wie verantwoordelijk is voor het omzetten van werkplekken per locatie, en hoe samenwerking plaatsvindt met interne ICT en eventuele huidige leveranciers.
IMP-14.	Migratie of herinrichting van accounts en toegang wordt zodanig uitgevoerd dat in-, door- en uitstroom niet wordt onderbroken en dat de overgang aantoonbaar controleerbaar is.
IMP-15.	Datamigratie omvat minimaal mailboxen, agenda's en contactpersonen, SharePoint- en Teams-data inclusief rechtenstructuren waar van toepassing, en OneDrive-data. Migratie vindt gecontroleerd plaats met validatie op volledigheid, integriteit en toegankelijkheid.

IMP-16.	Werkplekken worden gemigreerd of opnieuw ingericht volgens afgesproken werkplekscenario's, met minimale verstoring van onderwijsprocessen. De aanpak omvat planning per locatie, communicatie, en een fallback- of herstelprocedure.
IMP-17.	Voor migraties is een cutover-aanpak ingericht met planning rondom schoolkalender, testmomenten, communicatie naar gebruikers en afspraken over terugval bij verstoring.
IMP-18.	Applicatiekoppelingen en SSO worden tijdens migratie zodanig ingericht dat gebruikers toegang behouden tot geprioriteerde applicaties en dat wijzigingen vooraf worden afgestemd met betrokken leveranciers.
IMP-19.	Migratie wordt pas als afgerond beschouwd na acceptatie op basis van afgesproken acceptatiecriteria, inclusief een migratie-eindrapport met scope, afwijkingen, openstaande punten en beheerimplicaties.
IMP-20.	OPDRACHTNEMER levert een RACI-matrix waarin per activiteit en per dienstonderdeel is vastgelegd wat OPDRACHTNEMER doet en wat door de aanbestedende dienst of derden wordt uitgevoerd, voor zowel implementatie als beheer, inclusief afhankelijkheden en benodigde inzet vanuit de organisatie.
IMP-21.	OPDRACHTNEMER levert een communicatieplan per doelgroep (leerling, docent, ouder, medewerker, beheer) met ten minste planning, communicatiemomenten, verantwoordelijkheden en contenttemplates.

Informatiebeveiliging en Privacy

Eis-ID	Eis
IBP-1.	Security baselines voor de in scope omgeving zijn vastgesteld, toegepast en beheerst conform het Architectuurkader, inclusief expliciet beheer van afwijkingen en uitzonderingen binnen centrale governance.
IBP-2.	De Oplossing moet opgezet en geleverd worden vanuit het basisprincipe “Secure-by-Design”.
IBP-3.	OPDRACHTNEMER heeft informatiebeveiliging en continuïteit aantoonbaar gestructureerd en gestandaardiseerd, en tevens een continue en procesmatige PDCA cyclus ingericht, op alle lagen van haar eigen organisatie (inclusief betrokken onderaannemers) en die van de Dienstverlening.
IBP-4.	De Dienstverlening en organisatie van de OPDRACHTNEMER moet zijn beveiligd door het implementeren en onderhouden van een set van passende technische en organisatorische maatregelen welke de beschikbaarheid, integriteit en vertrouwelijkheid van de oplossing en de daarop opgeslagen en/of verwerkte informatie borgt op ten minste industriestandaard wijze.
IBP-5.	Voor het uitvoeren van onderhoud en/of aanpassingen van de Dienstverlening moet aantoonbaar een wijzigingsproces gehanteerd worden (“change management”) waarbij de nadruk ligt op het voorkomen van beveiligingsincidenten, storingen of onderbrekingen tijdens het doorvoeren van veranderingen.
IBP-6.	OPDRACHTNEMER draagt zorg dat software die onderdeel is van de Oplossing gedurende de looptijd wordt ondersteund door de betreffende leverancier en aantoonbaar blijft functioneren binnen de SRL-werkomgeving, inclusief tijdige opvolging van end-of-life/end-of-support en compatibiliteitswijzigingen.
IBP-7.	OPDRACHTNEMER meldt informatiebeveiligingsincidenten, waaronder maar niet beperkt tot datalekken, direct en in ieder geval binnen 24 uur per e-mail bij OPDRACHTGEVER.
IBP-8.	In het geval van een informatiebeveiligingsincident moet OPDRACHTNEMER direct maatregelen treffen om de gevolgen en de schade te beperken voortkomend uit het incident.
IBP-9.	OPDRACHTNEMER (incl. onderaannemers) verleent medewerking bij het onderzoeken en oplossen van een informatiebeveiligingsincident en stelt, indien gevraagd, alle relevante informatie met betrekking tot het incident (binnen de scope van de Dienstverlening) ter beschikking aan OPDRACHTGEVER. Deze informatie blijft minimaal zestig (60) dagen na het afhandelen van het incident beschikbaar en wordt desgevraagd ook beschikbaar gesteld voor onderzoek door een door OPDRACHTGEVER aangewezen derde.
IBP-10.	OPDRACHTNEMER heeft monitoring-, meld- en responsprocedures geïmplementeerd (en evalueert periodiek de effectiviteit daarvan) om informatiebeveiligingsincidenten (waaronder datalekken m.b.t. persoonsgegevens) te detecteren, melden en de gevolgen daarvan te mitigeren.
IBP-11.	Gegevens van OPDRACHTGEVER zijn altijd logisch en functioneel gescheiden van die van de overige afnemers c.q. klanten van OPDRACHTNEMER.
IBP-12.	De oplossing versleutelt alle gegevens, waarbij gebruik gemaakt wordt van de geldende ‘best practices’ (afhankelijk van de stand der techniek) m.b.t. versleuteling.
IBP-13.	OPDRACHTNEMER beschikt over aantoonbaar sleutelbeheer (key management) waarmee encryptiesleutels kunnen worden geroteerd en, waar technisch mogelijk, ingetrokken of ongeldig gemaakt conform procedures.

IBP-14.	SRL wordt geïnformeerd over de eventuele gebleken tekortkomingen m.b.t. beveiliging n.a.v. de door haar ingestelde beveiligingstest/-audits of onderzoek ihkv de Dienstverlening en deze dienen meegenomen te worden bij de doorontwikkeling van de Oplossing en zo nodig op de kortst mogelijke termijn te worden gepatcht.
IBP-15.	Alle medewerkers van de OPDRACHTNEMER die participeren in de levering van de Dienstverlening moeten aantoonbaar bekend zijn met de verantwoordelijkheid op het gebied van informatiebeveiliging en privacy die als onderdeel van zijn / haar rol van toepassing zijn.
IBP-16.	OPDRACHTNEMER draagt zorg dat alle medewerkers die participeren in de levering van de Dienstverlening een geheimhoudingsovereenkomst ondertekenen en hiernaar handelen.
IBP-17.	Malicieuze activiteiten worden gesignaleerd, gerapporteerd en gelogd in het logbestand.
IBP-18.	OPDRACHTNEMER stelt OPDRACHTGEVER in staat om aan te tonen dat er betrouwbare, effectieve en controleerbare mechanismen worden ingezet voor het vastleggen en vaststellen van de identiteit van gebruikers, (en het toekennen van rechten aan gebruikers bij het gebruik van de Dienstverlening) door gebruikers. Onder gebruikers worden hier, en in de overige IBP eisen, verstaan alle Medewerkers die op enige wijze gebruik maken van de Dienstverlening of toegang hebben tot de Oplossing.
IBP-19.	De Dienstverlening moet afdwingen dat gebruikers alleen toegang hebben tot informatie, beheertaken en speciale bevoegdheden voor zover dat voor de uitoefening van de werkzaamheden noodzakelijk is (“need to know”, “need to use”, “least privilege”) en ze hiervoor herleidbaar geautoriseerd zijn.
IBP-20.	Als er (bijzondere) persoonsgegevens in het systeem staan, dient het gebruik van multifactor authenticatie afgedwongen te worden.
IBP-21.	Als medewerkers van de OPDRACHTNEMER in enige vorm toegang hebben tot (bedrijfs)gegevens van OPDRACHTGEVER, dient het gebruikersaccount tenminste te zijn voorzien van multifactor authenticatie.
IBP-22.	OPDRACHTNEMER is verantwoordelijk voor het periodiek (minimaal eens per kwartaal) controleren van de toegangsrechten van Medewerkers die werkzaamheden uitvoeren ten behoeve van de Dienstverlening.
IBP-23.	OPDRACHTNEMER stelt een vaste contactpersoon aan die voor de Dienstverlening verantwoordelijk is voor zowel informatiebeveiliging als privacy.
IBP-24.	OPDRACHTNEMER moet zorgen voor een rapportage waarmee verantwoording wordt afgelegd over de mate van invulling en effectiviteit van de getroffen beveiligingsmaatregelen en het gerealiseerde beveiligingsniveau (inclusief privacy) binnen de scope van de Dienstverlening.
IBP-25.	Patch management moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de Dienstverlening en borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd.
IBP-26.	Patchmanagement is ingericht met concrete doorlooptijden per type patch (waaronder kritieke beveiligingspatches), inclusief rapportage over naleving en afwijkingen, zodanig dat kwetsbaarheden tijdig worden gemitigeerd zonder verstoring van onderwijscontinuïteit.
IBP-27.	Penetratietesten moeten procesmatig en procedureel, ondersteund door richtlijnen, worden uitgevoerd op alle ICT-componenten van de Oplossing.
IBP-28.	OPDRACHTNEMER rapporteert in het kader van de Dienstverlening de resultaten van de penetratietesten direct aan OPDRACHTGEVER en legt vervolgens periodiek (minimaal eens per kwartaal) verantwoording af over de opvolging van de bevindingen.

IBP-29.	De Dienstverlening moet gedurende de gehele looptijd van de Overeenkomst voldoen aan de algemene vigerende wet- en regelgeving van de Nederlandse overheid, waaronder de Algemene Verordening Gegevensbescherming (AVG).
IBP-30.	In lijn met de Verwerkersovereenkomst verwerkt OPDRACHTNEMER persoonsgegevens uitsluitend op basis van schriftelijke instructies van OPDRACHTGEVER en uitsluitend voor doeleinden die rechtstreeks voortvloeien uit de overeenkomst. Verwerking voor test- of analyse-doeleinden vindt alleen plaats indien dit noodzakelijk is voor de uitvoering van de dienstverlening, vooraf schriftelijk is afgestemd met OPDRACHTGEVER en bij voorkeur met geanonimiseerde of gesynthetiseerde gegevens.
IBP-31.	Daar waar OPDRACHTGEVER geen volledige toegang heeft tot de persoonsgegevens moet OPDRACHTNEMER OPDRACHTGEVER ondersteunen bij verzoeken tot inzage, correctie en eventueel het wissen van persoonsgegevens.
IBP-32.	De Dienstverlening moet de mogelijkheid bieden om gegevenscomponenten die niet strikt noodzakelijk zijn voor latere verwerkingen of waarvoor geen doelbinding of rechtsgrond aanwezig is, te verwijderen.
IBP-33.	Bij toepassing van data-protection-by default door OPDRACHTNEMER moeten tenminste de volgende aspecten meegewogen worden: 1. Beperk zoekfunctionaliteit m.b.t. persoonsgegevens en geef alleen zoekresultaten weer na het invoeren van een aantal persoonsgegevens. 2. Pas whitelisting toe voor het opvragen van persoonsgegevens. De sterkte van whitelisting is afhankelijk van de implementatie van de whitelist. Een goede toepassing is dat de whitelist wordt samengesteld door een mechanisme/tooling die onafhankelijk is van de gebruiker (bv. een workflow-systeem waarmee de gebruiker alleen toegang krijgt tot persoonsgegevens van de betrokkene waar hij op dat moment mee bezig is).
IBP-34.	Tijdelijke bestanden e/o logs met betrekking tot de Dienstverlening moeten zo min mogelijk persoonsgegevens bevatten in de productie-omgeving. OPDRACHTNEMER dient dit periodiek te evalueren. Een BSN mag in ieder geval nooit in logbestanden van OPDRACHTNEMER voor komen.
IBP-35.	OPDRACHTNEMER heeft procedures om analyseren van risico's te borgen in het kader van de Dienstverlening. De (opvolging van de) voor OPDRACHTGEVER relevante (IB)-risico's en mitigerende maatregelen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met OPDRACHTGEVER afgesproken rapportagecyclus.
IBP-36.	OPDRACHTNEMER legt bekende risico’s vast in een register en deze wordt door OPDRACHTNEMER voorzien van de nodige (borgings-)maatregelen ter mitigatie van de risico’s.
IBP-37.	Security hardening moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de Oplossing.
IBP-38.	OPDRACHTNEMER hanteert internationaal erkende security hardening standaarden, (bijv: Center of Internet Security (CIS) benchmarks, als basis voor het vaststellen van de security hardening richtlijn voor de ICT-componenten.
IBP-39.	Beveiligingsrelevante activiteiten binnen de Oplossing en de beheerhandelingen worden gelogd conform een logging- en monitoringbeleid (use cases, retentie, toegangsbeheer en rapportage), passend bij het informatiebeveiliging- en privacybeleid.
IBP-40.	De logbestanden kunnen niet achteraf worden aangepast.
IBP-41.	OPDRACHTNEMER heeft een procedure waar wordt geborgd dat continu naar nieuwe kwetsbaarheden en dreigingen wordt gezocht (vulnerability management) in het kader van regulier beheer en bij in gebruik name van een nieuwe dienst/ICT-component/significante wijziging. De (opvolging van de) voor OPDRACHTGEVER relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met OPDRACHTGEVER afgesproken rapportagecyclus.

IBP-42.	OPDRACHTNEMER moet borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd en zorgt dat installatie van nieuwe patches geen afbreuk doet aan de continuïteit en beschikbaarheid van de Dienstverlening.
IBP-43.	Voor ingebruikname van een nieuwe dienst / ICT-component en bij een significante wijziging van de Oplossing moet een kwetsbaarhedenscan uitgevoerd worden en moeten de bevindingen opgelost worden.
IBP-44.	OPDRACHTNEMER dient bij het ontwikkelen, implementeren en beheren van de Dienstverlening de principes "Security by Design and default" (secure software development) en “Privacy by Design and Default" toe te passen.
IBP-45.	OPDRACHTNEMER beschikt over passende en aantoonbare maatregelen en beleid zodat de Dienstverlening voldoet aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties
IBP-46.	OPDRACHTNEMER beschikt over passende en aantoonbare maatregelen en beleid om de op basis van de OWASP top tien (https://owasp.org/www-project-top-ten/) meest kritische beveiligingsrisico’s binnen een webapplicatie te vermijden voor wat betreft de Dienstverlening.
IBP-47.	In het kader van opslag en/of transport van persoonsgegevens moet de Oplossing voldoen aan de cryptografische beveiligingsvoorzieningen zoals voorgeschreven in de NCSC ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS). https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
IBP-48.	OPDRACHTNEMER moet een procedure hebben, uitvoeren en de resultaten rapporteren voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de Dienstverlening.
IBP-49.	Alle Koppelingen tussen de Oplossing en bron-en doelsystemen van OPDRACHTGEVER moeten op basis van open standaarden 'comply or explain' plaatsvinden.
IBP-50.	Bij multi-tenancy worden alle gegevens die binnen de Oplossing worden opgeslagen of verwerkt ten behoeve van OPDRACHTGEVER versleuteld en gescheiden verwerkt op gehardende (virtuele) machines.
IBP-51.	Gestructureerd en periodiek dient overleg tussen OPDRACHTNEMER en OPDRACHTGEVER plaats te vinden om zowel de rapportages als (eventuele) issues te bespreken.
IBP-52.	OPDRACHTNEMER moet OPDRACHTGEVER direct op de hoogte stellen van risico’s die de classificatie “hoog” bestempeld krijgen.
IBP-53.	Voor de Dienstverlening is verwijdering ingericht (o.a. in het kader van bewaartermijnen) met betrekking tot tijdelijke bestanden en/of logs waarin persoonsgegevens voorkomen. Deze bestanden/logs worden niet langer bewaard dan maximaal dertien (13) maanden, tenzij wet- of regelgeving een langere termijn vereist.
IBP-54.	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen moeten regelmatig worden gemonitord (bewaakt, geanalyseerd) en de bevindingen periodiek gerapporteerd als onderdeel van het informatiebeveiliging incidentenproces.

Teams en Sharepoint

Eis-ID	Eis
TS-1.	OPDRACHTNEMER beheert de Teams-omgeving actief conform afspraken (aanmaakbeleid, naamgeving, eigenaarschap, lifecycle, gasttoegang en periodieke opschoning) en rapporteert hierover conform de rapportagecyclus.
TS-2.	OPDRACHTNEMER beheert de SharePoint-omgeving actief conform afspraken (site-aanmaak, permissies, deling, lifecycle, template-gebruik en periodieke opschoning) en rapporteert hierover conform de rapportagecyclus.
TS-3.	OPDRACHTNEMER ondersteunt OPDRACHTGEVER bij het inrichten van een leeromgeving binnen SharePoint door het leveren van technische inrichting, templates en beheerafspraken. Inhoudelijke invulling (content) ligt bij OPDRACHTGEVER, tenzij expliciet anders overeengekomen
TS-4.	OPDRACHTNEMER faciliteert per locatie een digitale communicatieomgeving (bijv. SharePoint intranet/site) voor nieuws en interne informatie, inclusief standaardtemplate, rechtenstructuur en beheerafspraken.

Exit

Eis-ID	Eis
EX-1.	OPDRACHTNEMER levert bij contracteinde op een exit-aanpak die beschrijft hoe overdracht naar een opvolgend leverancier of interne beheerorganisatie wordt ondersteund zonder verstoring van onderwijsprocessen.
EX-2.	Configuraties, beleidssets en inrichtingsoverzichten van de in scope omgeving zijn overdraagbaar en worden zodanig gedocumenteerd dat een opvolgend partij beheer kan overnemen.
EX-3.	OPDRACHTNEMER ondersteunt overdracht van identiteits- en toegangsconfiguraties,
EX-4.	OPDRACHTNEMER ondersteunt overdracht van endpoint management inrichting, inclusief policysets, applicatiecatalogus en baselines, zodat beheerde werkplekken beheersbaar blijven bij overgang.
EX-5.	Bij contracteinde ondersteunt OPDRACHTNEMER kennisoverdracht, inclusief overdrachtssessies, runbooks en een actuele contact- en escalatiestructuur.
EX-6.	Tijdens de exitperiode blijft OPDRACHTNEMER beheer en ondersteuning leveren conform de afgesproken serviceafspraken totdat overdracht is afgerond of anders overeengekomen.
EX-7.	Bij exit worden toegangen, accounts en rechten van OPDRACHTNEMER en onderaannemers aantoonbaar ingetrokken en wordt dit vastgelegd.
EX-8.	De inrichting en documentatie ondersteunen een soepele overstap door gebruik van standaarden en herleidbare configuraties, waarbij afhankelijkheden expliciet zijn vastgelegd.
EX-9.	Bij einde overeenkomst toont OPDRACHTNEMER op verzoek van OPDRACHTGEVER aan dat alle gegevens van OPDRACHTGEVER die zich bij OPDRACHTNEMER (en onderaannemers) bevinden, zijn geretourneerd en/of vernietigd conform de verwerkersovereenkomst en toepasselijke bewaartermijnen. Indien OPDRACHTGEVER geen verzoek doet, verstrekt OPDRACHTNEMER uiterlijk binnen twaalf (12) maanden na einde overeenkomst een verklaring van vernietiging/retentie conform DPA